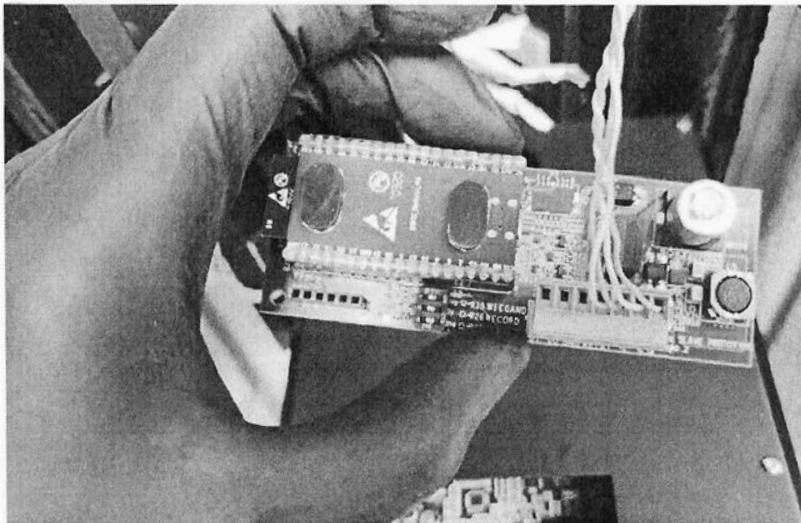


Case 1:21-cv-09321-JGK-VF Document 14 Filed 01/24/22 Page 43 of 86



409-112. At one building in Manhattan, GateGuard discovered this “extender” device inserted and connected inside GateGuard’s intercom. The picture shown below is the back of a portion GateGuard’s intercom. The extender device has been wedged onto Gateguard’s blue circuit board; the green strip connecting the extender wires to a separate Amazon device can be seen on the bottom right and the grey “bubbles” that can be seen on the upper left-hand portion of the extender depicted above can be seen on the upper right-hand side of GateGuard’s case below:

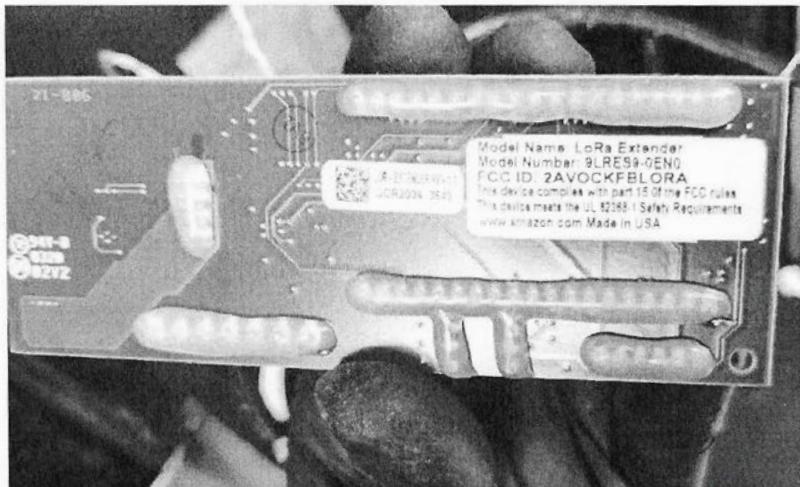
| Case 1:21-cv-09321-JGK-VF Document 14 Filed 01/24/22 Page 44 of 86



440-113. By connecting its device into the GateGuard intercom, Amazon can illegally “free- ride” off of GateGuard’s product while being placed on or near GateGuard’s circuitry resulting in malfunctioning that is blamed on GateGuard.

444-114. The dangerous placement of Amazon’s unauthorized device can be clearly seen in paragraphs 108 and 109. Circuit boards are incredible delicate electronics which are protected by cases and should not have even the tiniest unauthorized objects – let alone an entire alien circuit board – pressed against them. The insertion of the smallest objects on top of a circuit board cause an electric short, a broken part, or other permanent injury to the board. In this case, by wedging its “extender” into GateGuard’s case, Amazon damaged GateGuard electronic components, irreparably destroying the intercom screen.

Case 1:21-cv-09321-JGK-VF Document 14 Filed 01/24/22 Page 45 of 86



113. The “extension” benefits Amazon when the device does not malfunction and harms GateGuard when it does, by shorting its device, damaging the intercom screen, and disabling other electronic components.

114. The “extender” is clearly connected to the Amazon Key for Business device, as shown by the sticker on the reverse of the device identifying the model name, number and FCC ID, as well as the amazon.com website specifying ownership of the product.

115. The FCC ID clearly identifies Amazon.com Services Inc. as the “applicant/grantee”, as shown below:

Case 1:21-cv-09321-JGK-VF Document 14 Filed 01/24/22 Page 46 of 86

[Equipment Authorization Approval Guide](#)
[Approval Procedures](#)
[Measurement Procedures](#)
[Grantee Code](#)
[Importation](#)
[Knowledge Database](#)

[FCC ID Search](#)

[Equipment Authorization System](#)
[Testing Laboratory Search](#)
[Telecommunications Certification Body Search](#)
[Mutual Recognition Agreements](#)
[RF Device](#)
[FCC Rules \(Title 47\)](#)
[Testing Laboratory Qualifications](#)
[Other Information Sources](#)

FCC ID Search Form

Help
Advanced Search

Grantee Code (First three or five characters of FCCID)

Product Code (Remaining characters of FCCID)

search

Advanced Search

To perform an advanced search go to: <http://apps.fcc.gov/actfcreports/GenericSearch.cfm>. The advanced search permits search on a wide range of fields associated with an FCC ID to help find the information on a grant of certification.

FCC ID Search Instructions

- FCC ID numbers consists of two elements, a grantee code and an equipment product code. An FCC ID is assigned to all devices subject to certification.
- The grantee code, the first portion of the FCC ID, is either a three or five character alphanumeric string representing the Grantee Applicant.
- Grantee codes that begin with an alphabetic character (A-Z) of three characters in length. The second and third characters may be numbers or alphabetic characters.
- Grantee codes that begin with a number (2-9) are five characters in length. The second through fifth characters may be numbers or alphabetic characters.
- The grantee code does not contain numbers "one" and/or "zero". The grantee code is assigned by the Commission permanently to a company for authorization of all radio frequency equipment.
- The product Code is the second portion of the FCC ID that begins after the grantee code. The product code may include hyphens and/or dashes (-). The product code is assigned by the Grantee.
- More examples and some additional explanation is available on the FCCID help section.

1 results were found that match the search criteria:
Grantee Code: ZAVOC Product Code: KFBLORA

Displaying records 1 through 1 of 1.

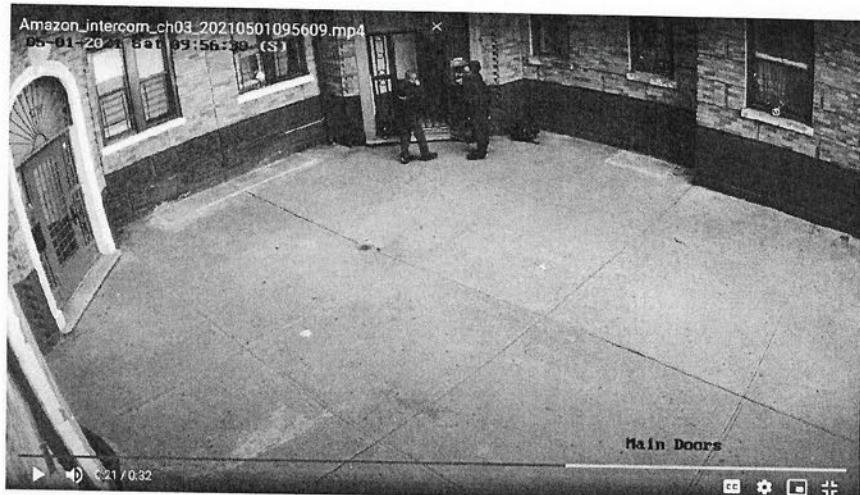
View Form	Display Exhibits	Display Grant	Display Correspondence	Assignee SAMS	Address	Site	State/Country	Etc. Code/ECC ID	Authorization	Final Action Date	Last FCC ID Change	Last FCC ID
Detail	Summary	Grant	Correspondence	SAMS	Amazon.com Services, Inc. 110 Terry Ave. North Seattle, WA 98109	United States	ZAVOCKFBLORA	Change in Identification 01/03/2019 02:31	927.5	2019-01-03 00:00:00	2019-01-03 00:00:00	

[Return to Search Results](#)

116. In addition, GateGuard has captured video of Amazon technicians tampering with multiple GateGuard devices.²² Set forth below are images from the video showing Amazon technicians after they illegally opened the GateGuard® device without authorization and destroyed it:

²² <https://drive.google.com/file/d/1sFIE7808kHtjKajLsomDTwzTl3w1zlic/view>
<https://drive.google.com/file/d/1Xtry9xVKCv1-VRr2NygpNvvDV03XjT4L/view>

Case 1:21-cv-09321-JGK-VF Document 14 Filed 01/24/22 Page 47 of 86



Case 1:21-cv-09321-JGK-VF Document 14 Filed 01/24/22 Page 48 of 86



Case 1:21-cv-09321-JGK-VF Document 14 Filed 01/24/22 Page 49 of 86

117. In the videos, Amazon employees wearing the jacket with the familiar Amazon prime half-moon ascending arrow logo can be seen installing a device into the existing intercom at a building served exclusively by GateGuard. Amazon did not obtain the consent of either GateGuard or the property owner for the installation of its Key.

Amazon's Key for Business Installations Routinely Damage Intercoms, Door Locks, and Wiring

118. On approximately 20 different occasions, building management have called GateGuard to repair or replace disabled intercom devices. These calls cost GateGuard time and money in support and repair, and it is likely that there are many more incidents that are not reported, causing even greater disruption to customers and loss of business.



Case 1:21-cv-09321-JGK-VF Document 14 Filed 01/24/22 Page 50 of 86



120. Each time GateGuard has been called by building management, GateGuard has discovered that Amazon tampered with its intercoms, including by inserting and connecting Amazon's extenders, a crucial component of the Key for Business "upgrade" responsible for the damage described above.

121. On information and belief, Amazon's actions are not isolated instances, but are systematic business practices designed to destroy competition. The numerous on-line complaints and the confirmation that Amazon representatives lie about their authority to install equipment as discussed above provide a reasonable inference that Amazon's practices are widespread.

122. Amazon's strategy is then to disparage its competitors' device – that it has itself damaged, but without the property owners' consent – and propose the Amazon Key as an "upgrade" to a system "degraded" by the Key itself.

123. As shown in the Twitter dialogue reproduced below, when installing Key for Business – with or without authorization from building management – Amazon routinely disables or destroys existing intercom devices, door locks, and wiring:

Case 1:21-cv-09321-JGK-VF Document 14 Filed 01/24/22 Page 51 of 86



2020

@1morequestion99

Replying to @MGTalksRetail @chriscantino and 3 others

Amazon installed their KFB system on our building and destroyed our display unit. Now the account manager won't return calls/emails. 😠😡

10:41 AM · Jan 28, 2021 · Twitter for iPhone



lane baysden

@lanebaysden

@AmazonHelp can you help me? Amazon Key installer damaged our building's call box and is now inoperable. Trying to figure out next steps and timeline.

6:03 PM · Nov 6, 2020 · Twitter for iPad

1 Retweet 1 Like



Amazon Help @AmazonHelp · Nov 6

Replying to @lanebaysden

We're sorry to hear this! We'd like to look into this. When you have a moment, please fill as much information as possible here: amzn.to/36gm8hG. Please let us know when you've completed the form, and we'll confirm we've received your details! ^KV



→□ All I want for Christmas is to be off of the Amazon Key call list.

Tweet It messed up our intercom system. We made them remove it.

124. After Amazon began aggressively seeking to control the building access market, GateGuard has received dozens of complaints and has been able to prove that these are directly related to Amazon's conduct.

Case 1:21-cv-09321-JGK-VF Document 14 Filed 01/24/22 Page 52 of 86

125. As discussed below, GateGuard has confronted Amazon with evidence of its misconduct and, rather than compensating GateGuard for the damage caused, on information and belief, Amazon has profited from the information provided by GateGuard to surreptitiously reinstall its devices to cover up its initial illegal tampering. On information and belief, all of the customer complaints relating to GateGuard devices failing after an Amazon Key installation are a direct result of Amazon's conduct. In addition, many instances of illegal installation remain undiscovered, continuing to put GateGuard's equipment at risk (because some devices short repeatedly and only fail over time) and continuing to provide Amazon with unearned benefits from its illegal free-riding conduct.

126. As a result of Amazon's conduct, a number of GateGuard customers, residents and others have come to believe falsely that GateGuard's intercom systems are defective or that they are otherwise less desirable or valuable to building owners than the Amazon systems that have been illegally inserted into GateGuard intercoms. When the Key does not damage or destroy the device, Amazon also profits from its illicit activities.

Amazon Attempts to Avoid Detection

127. To prevent detection, particularly after it learns that a savvy access control provider such as GateGuard has become aware of its tactics, Amazon removes its "extenders" from GateGuard's devices after they have been sufficiently damaged.

128. GateGuard has been told by building managers that Amazon misleads them, claims the extenders had nothing to do with any malfunctioning of GateGuard's devices and then returns to the building to install a new device that it now presents as an "update" that will avoid the problems with the previous access control system. Since the property managers were in many, if not most situations, unaware of the initial installation, they can easily be duped by Amazon. Even

Case 1:21-cv-09321-JGK-VF Document 14 Filed 01/24/22 Page 53 of 86

in rare situations where the property managers authorized the installation, they were not informed of the manner in which Amazon would install its Key directly into GateGuard's intercom or onto its wiring, leading the property managers to believe Amazon's lies that their product had nothing to do with GateGuard's malfunctioning. Landlord's properties' have also been damaged, as building amplifiers are blown out and the building magnetic door strikes are disabled by the surreptitious installation of the Key without property owners', and managers', knowledge and consent.

129. As a result of Amazon's conduct, GateGuard has suffered reputational harm, diminished customer loyalty, and loss of revenue and other valuable commercial relationships, both existing and prospective.

Amazon Reveals its Intentions

130. In October of 2020, GateGuard approached Amazon and provided considerable evidence of its destructive and unlawful conduct (including the evidence incorporated above).

131. In addition to denying any responsibility for its conduct, Amazon "gaslit" GateGuard, suggesting that the failure of GateGuard devices identified as having been the result of tampering by Amazon was not because of anything done by Amazon but, rather, was GateGuard's fault.

132. Amazon's arguments to this effect, however, were unsubstantiated, unsupportable and false.

133. Although Amazon evinced interest in further discussions to explore a potential resolution, when the parties met, Amazon refused to cease installing Key for Business in a manner that damaged GateGuard and merely offered to enlist GateGuard as a Key for Business installer, for which GateGuard would be paid a nominal fee.

Formatted: Font: Bold, Font color: Red, Complex Script
Font: Bold

Formatted: Font: Bold, Font color: Red, Complex Script
Font: Bold

Formatted: Font: Bold, Font color: Red, Complex Script
Font: Bold

Formatted: Font: Bold, Font color: Red, Complex Script
Font: Bold

Formatted: Font: Bold, Font color: Red, Complex Script
Font: Bold

Case 1:21-cv-09321-JGK-VF Document 14 Filed 01/24/22 Page 54 of 86

134. Amazon characterized the Hobson's choice it presented to GateGuard (which was recorded on video by GateGuard) along the lines of, "either [Amazon] can cost you money or make you money." This is exactly the strategy Amazon aims to deploy with other potential rivals,

turning itself into the essential gatekeeper, relegating third parties, at best, to an “adjunct” role and making it prohibitively expensive for others to provide rival and truly competitive access solutions. In the long run, this strategy aims not only to control the access market, but, ultimately, to control the ecommerce and package delivery markets generally.

Amazon Takes Its Theft of GateGuard's Trade Secrets Into Overdrive by Stealing the Intellectual Property Behind the Entire GateGuard System.

Formatted: Font: Bold, Italic, Complex Script Font: Bold, Italic
Formatted: Font: Italic, Complex Script Font: Italic
Formatted: Font: Italic, Complex Script Font: Italic
Formatted: Left, Indent: Before: 0.13", Line spacing: single

135. Not content to break into GateGuard's devices to observe their inner workings and modify the Key so that it would be “compatible” with GateGuard – without GateGuard's consent and in violation of GateGuard's Terms and Conditions – on or about March 8, 2023, Amazon instructed one of its channel partners to pose as a GateGuard client and obtain two devices for inspection by Amazon.

136. Amazon further instructed its channel partner to ship one device to the A2Z Development ^{‘enter’²} and to ship one device to .

137. Once the device had been acquired, GateGuard naturally activated the device.

138. Thus by posing as a client, the channel partner was able to provide Amazon with an activated device that its engineers could use to hack into the GateGuard “back end” and thus observe the functioning of the GateGuard system as a whole, an not merely the functioning of the GateGuard intercom itself, that enables property management at residences under contract to GateGuard.

Formatted: Font: Bold, Complex Script Font: Bold

139. After examining, analyzing, and testing the GateGuard device, the Key for Business rolled out a new service, transforming the Key device from a door unlocking service for Amazon deliverers to a property management tool for property managers. Amazon is thus using its

knowledge of the GateGuard system specifically to target the customers of GateGuard and others serving the property management market.

140. The new service is specifically defined by Amazon as a “web-based portal for property managers to manage third party provider access,” as described in more detail in paragraph 12 above. This service closely parallels GateGuard’s Property Panel, available as part of the GateGuard system that Amazon had access to at its research and development center after the device was shipped to the center in March 2021.

141. Most importantly, at the time that Amazon illegally acquired one of GateGuard’s activated devices and sent it to its secret Ring-controlled research laboratory, Rin:

. Ring was able to observe the functioning of the GateGuard devices and modify the Ring Intercom to incorporate elements of the GateGuard system and also refine the integration of its Ring Intercom that was designed for the European market where a device such as the Ring Intercom would need to integrate with a wide variety of existing intercom systems. Naturally, Amazon did not inform GateGuard of its use of its device.

142. Instead, once Amazon had used the device for its own purposes, to definitively bury its tracks.

Commented [EQ1]: NB; Deleted: On information and belief.



Formatted: Left, Indent: Before: 0.5", No bullets or numbering

See what is going on at your door without opening the app.

Rich Notifications

Include snapshots in notifications.

[Learn More](#)

143. Set forth below are images showing the functioning of the later-introduced Ring “rich notification”.

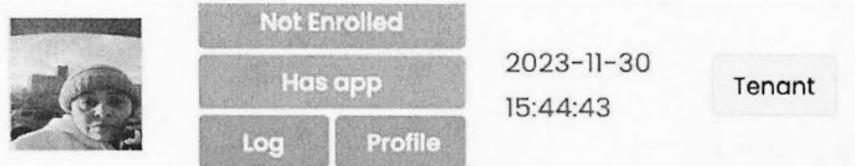
Formatted: Left

144. “When you receive a Rich Notification you will see a small image, this is the snapshot of the event. You can enlarge this directly from the push notification. As Amazon describes the feature:

145. Like Ring, GateGuard offers a “rich notification” feature to its users, developed before the Ring was introduced and with higher reliability and greater resolution.

146. Set forth below is an image of the GateGuard feature, showing the device video capture being sent as a still image to a user's mobile phone:

Formatted: Left, Indent: Before: 0", First line: 0.5", Numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 120 + Alignment: Left + Aligned at: -0.36" + Indent at: 0.14"

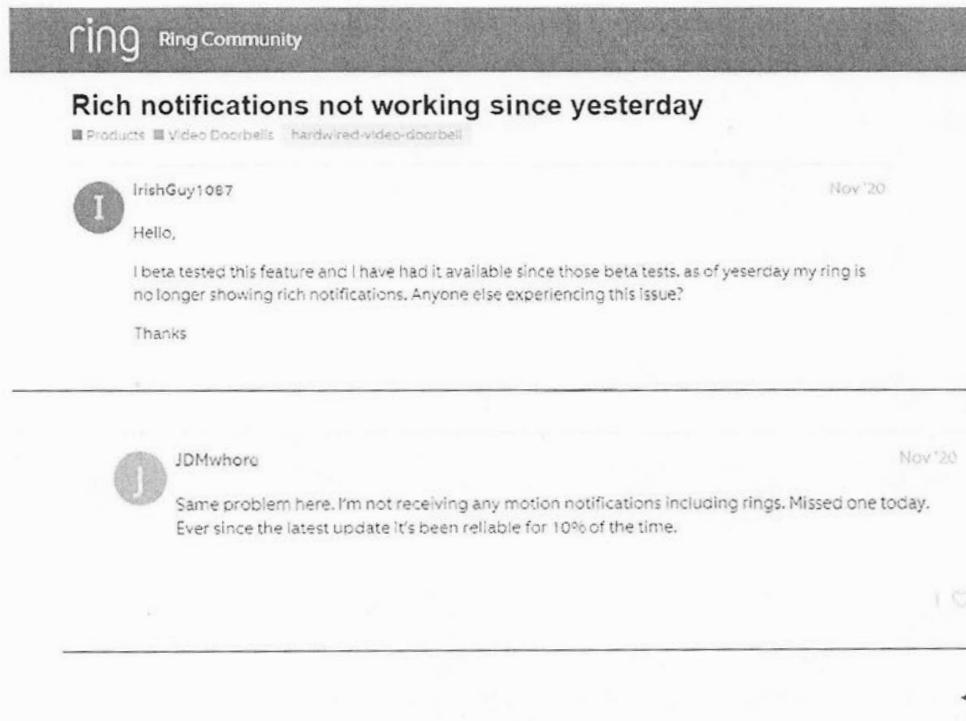


Larger view of image



147. However, Ring encountered numerous problems and "bugs" in its roll-out of the Ring, leading to

extensive consumer complaints. <https://community.ring.com/t/rich-notifications-not-working-since-yesterday/18722>.



The screenshot shows a post in the Ring Community forum. The post title is "Rich notifications not working since yesterday". The poster is "IrishGuy1067" (Nov '20). The post content: "Hello, I beta tested this feature and I have had it available since those beta tests, as of yesterday my ring is no longer showing rich notifications. Anyone else experiencing this issue? Thanks". Below the post, another user "JDMwhore" (Nov '20) responds: "Same problem here, I'm not receiving any motion notifications including rings. Missed one today. Ever since the latest update it's been reliable for 10% of the time." A note at the bottom right of the screenshot indicates "Formatted: Left, No bullets or numbering".

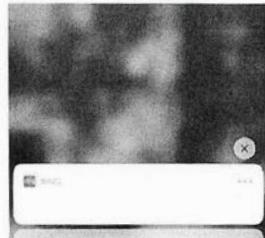
S

strulls

Apr '21

Formatted: Left, Indent: Before: 0.5"

I have found that rich notifications will work fine and then all of a sudden will go blank. This happened today. I'm wondering if it happens when there's an update to the app (like there was yesterday I believe). For reference, the issue looks like the attached image. Restarting the phone does seem to fix it without having to completely delete the app as suggested earlier.



Summary of Amazon's Anti-Competitive Conduct

435-148. Amazon is not achieving dominance of the building access and e-commerce delivery markets by technological innovation, but by deception, harassment, ruthlessness, and blatantly illegal conduct, such as the unauthorized accessing of and tampering with GateGuard and other parties' devices, and the pattern of lies and misrepresentations through which it deceives lower-level apartment personnel to permit installation of the Key without the need to contact and consult the "higher-ups."

436-149. The House Antitrust Report documents Amazon's brazenly anti-competitive behavior, highlighting Amazon's bullying, appropriation of third-party seller data, imposing fees on captive users of its platforms, "self-preferencing" and abusing its "gatekeeper power." Much of the House Antitrust Report evokes patterns strikingly similar to the conduct that has so damaged GateGuard, and underscores the anti-competitive purpose underlying Amazon's deceptive, illegal and cut-throat practices: "Once Amazon succeeds in trapping enough customers in its "flywheel" to secure dominant position across varied markets, it can then raise

Commented [EQ2]: Deleted stray comment : "By observing a"

Formatted: Left

Formatted: Left

prices or remove incentives or allowances for third party sellers/competitors.” Damning as it is, however, the House Antitrust Report is not the only source of information for Amazon’s history of anti-competitive practices.

437-150. Reuters recently reported that it had reviewed thousands of internal Amazon documents – including emails, strategy papers and business plans – that show the

Case 1:21-cv-09321-JGK-VF Document 14 Filed 01/24/22 Page 62 of 86

company ran a systematic campaign of creating knockoffs and manipulating search results to boost its own product lines in India, one of the company's largest growth markets. The documents reveal how Amazon's private-brands team in India secretly exploited internal data from Amazon.in to copy products sold by other companies, and then offered them on its platform.²³ On information and belief, Amazon has stolen GateGuard's proprietary data in a similar manner.

¶38-151. The conduct of which GateGuard and others have been victim in fact represents the anti-competitive DNA at the core of the Amazon business model.

CAUSES OF ACTION

COUNT I.

COMPUTER FRAUD AND ABUSE ACT (18 U.S.C. § 1030 *et seq.*) (AS TO ALL DEFENDANTS)

¶439-152. GateGuard realleges and incorporates by reference each and every allegation set above.

← Formatted: Left

¶440-153. GateGuard's devices are "high speed data processing device performing logical, arithmetic, or storage functions" and thus come within the definition of "computer" under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(e)(1).

← Formatted: Left

¶441-154. GateGuard's intercom devices are involved in interstate and foreign commerce because they control packages and other deliveries to residential dwellings that originate from locations both inside and outside of the State of New York. As a result, GateGuard's intercoms are "protected computers" under 18 U.S.C. § 1030(e)(2).

²³ <https://www.reuters.com/investigates/special-report/amazon-india-rigging/>

Case 1:21-cv-09321-JGK-VF Document 14 Filed 01/24/22 Page 63 of 86

| 442-155. Upon information and belief, Defendants knowingly and intentionally accessed
GateGuard's intercom devices without authorization or in excess of authorization, and thereby
obtained and used valuable information from those devices, including customer locations,
accounts, and id's, in violation of 18 U.S.C. § 1030(a)(2)(C).

Formatted: Left

| 443-156. Upon information and belief, Defendants intentionally accessed a protected
computer or computers without authorization, and as a result of such conduct, caused damage and
loss, in violation of 18 U.S.C. § 1030(a)(5)(C), or recklessly caused damage in violation of 18
U.S.C. § 1030(a)(5)(B).

| 444-157. Defendants caused loss to one or more persons during a one-year period
aggregating well over \$5,000 in value, and they also caused damage affecting ten or more protected
computers during a one-year period under 18 U.S.C. § 1030(c)(4)(A)(i)(I).

Formatted: Left

| 445-158. Amazon's imposition of ever-increasing delivery quotas as part of its illegal scheme
described herein poses a direct threat to public health and safety, harming both the drivers and
installers and also leading to reckless driving conduct, in violation of 18 U.S.C. §
1030(c)(4)(A)(i)(4).

| 446-159. GateGuard has suffered damage and loss as a consequence of Defendants' actions,
including but not limited to the cost of investigating and responding to unauthorized access and
abuse of its intercom devices, conducting damage assessments, restoring and replacing intercom
devices, wiring, systems, or information, termination of contracts, the loss of existing and future
business, the interference with GateGuard's uploading and preservation of proprietary data, and
the harm to GateGuard's operations, reputation and goodwill as described above, all in an amount
to be determined at trial, but no less than FORTY MILLION DOLLARS (\$40,000,000) together
with attorneys' fees and other equitable relief under 18 U.S.C. § 1030(g).